EXHIBIT 3

REDACTED PUBLIC VERSION

harborlabs

IOENGINE, LLC. V PAYPAL HOLDINGS, INC.,

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

Case No. 1:18-cv-452 WCB

EXPERT REPORT OF DR. AVI RUBIN REGARDING VALIDITY OF U.S. PATENT NOS. 9,059,969 AND 9,774,703

January 7, 2022

Respectfully submitted,

Dr. Aviel D. Rubin.

HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY – SOURCE CODE SUBJECT TO PROTECTIVE ORDER

specify DUKPT, such as ANSI X9.24-3 (2017), ANSI X9.24-1(2009), ANSI X9.24-1(2004) and earlier ANSI X9.24 versions, DUKPT (Derived Unique Key Per **Transaction**) is a key management mechanism mostly used in financial services, especially the payment industry. Patents referenced by Dr. Bims also recognize this fact. For example, U.S. Patent No. 5,764,789 referenced by Dr. Bims is titled "Tokenless biometric **ATM access system**"; U.S. Patent No. 5,613,012 is titled "Tokenless identification system for authorization of **electronic transactions** and **electronic transmissions.**" Patents referenced by Dr. Bims that do not address financial transactions in their titles also recognize DUKPT's financial attributes. For example, U.S. Patent No. 5,745,576 emphasizes that "DUKPT is described in ANSI standard X9.24 (see "**Financial Services** Retail Key Management" American National Standard for Financial Services ANSI/ABA X9.24-1992, pp 36-50, attached as Appendix A). DUKPT is a key management technique intended for encrypting and protecting PIN information during **transactions**."

C. Synchronization

47. I have reviewed Dr. Bims' opinions regarding synchronization and the state of the art circa 2001-2004. I disagree with Dr. Bims for at least the following reasons.

48. Fundamentally, Dr. Bims' definition of "synchronization" is wrong. Dr. Bims references his own patent, the '911 patent, which "teaches a synchronization methodology for aligning the transmission and reception of messages... across a medium... for example, synchronizing clock timers in the receiving and transmitting device to a common GPS time." [Bims, 120] However, following that statement, Dr. Bims contends that "this is not the same type of 'synchronization' in the Asserted claims," because the Asserted Claims refer to "synchronizing content," which would include "the prototypical example of files." [Bims, 120]

49. Dr. Bims demonstrates an incorrect understanding of "synchronizing content" to

the entent he defines it solely to be "file synchronization." Synchronization is not limited to "file synchronization," it can include synchronization of any type of data. A POSITA at the time of invention would interpret "synchronizing content" broadly to include the process for the synchronization of any set of data, which could be information, records, messages, statistics, etc., whether embedded in file formats or as files themselves. A POSITA would understand that "synchronizing content" as used in the context of the Patents-in-Suit requires a degree of automation. In other words, a process of manually copying files from one location to another or deleting files is not "synchronizing content." ['969 Patent at 6:32-48, 4:18-24

50. The asserted '703 and '969 patents also do not limit "synchronization" to just synchronizing files. For example, the '703 Patent mentions that "[i]f synchronization is specified 470, then the TCAP will provide and receive updated data to and from the backend server, overwriting older data with updated versions of the data 475." ['703, 8:46-51]. The '703 Patent does not specify that such data must be complete files or contained within files. The '703 Patent also addresses synchronization of other information, including "options 770 for advertising 780, events 775, promotions 772, and/or the like." ['703, 12:50-57] The '703 Patent also does not require these components to be in a file or in any particular format. Similarly, the '703 Patent also specifies "synchronizing data" and "synchronizing program code" in Claims 25-26, without specifying that these components must be in files.

V. SUMMARY OF THE PATENTS-IN-SUIT

A. The '703 Patent

51. The '703 patent is titled "Apparatus, Method, and System for a Tunneling Client Access Point." It describes a solution to securely access, execute, and process data in a compact, portable form. In essence, the invention is a portable device referred to as a Tunneling Client

15:2-4, 16:17-22]. However, Abbott's LIBDOC program does not involve synchronizing because it describes manual operations. The exemplary data-synchronizing described in the '703 Patent is an automated process involving receiving updated data (e.g., from a server) and overwriting old data in the portable device memory with the updated data. '703 Patent 8:48−51, 9:53−58, 19:50−55, 27:55−58. To the contrary, as cited by Dr. Bims in paragraph 735, LIBDOC "allows a secure document librarian to grant access to documents," and allows the "trusted librarian [to] update the personal key." [Abbott, 16:17−22]. The fact that a librarian could save or erase information of his or her own choosing is not what a POSITA would understand as the claimed "synchronization." And nowhere is there any disclosure of synchronization between the portable device and the server. Similarly, Abbott at 16:29-40 and 14:44-46 teaches only that documents can be decrypted and viewed by a user if the personal key 200's secret is correct; it does not teach a synchronization process from the portable device to the server.

408. In addition, Dr. Bims does not identify any content on the portable device that is being synchronized. Dr. Bims mentioned emails and documents, but both items reside on the terminal, not the portable device.

b. Abbott in Combination with Shmueli Does Not Disclose "Facilitat[ing] Synchronizing Content on the Portable Device with Content on the Communications Network Node"

409. As I discussed in Section IX.C.i.b above, I disagree with Dr. Bims that it would have been obvious for a POSITA to combine Abbott with Shmueli.

410. Regardless, Shmueli does not teach this claim element. Dr. Bims references a backup procedure, such that "level 1 security may correspond to those keylets requiring higher levels of security or privacy, such as those containing transactional information or passwords. As such, the corresponding keylets may only store data on the key 10 and only backup the information

to web-based services through secure interaction." [Shmueli, 0089]. Shmueli specifies two separate actions for these keylets: 1) saving files to the portable device, and 2) backing up information to web-based services. These two separate actions do not indicate that content on the portable device is being synchronized with content on the network communications node. As I explained earlier, a POSITA would understand that "synchronizing content" requires a degree of automation. In other words, a process of manually copying files from one location to another or deleting files is not "synchronizing content."

411. In addition, Dr. Bims does not identify how program code on the portable device is executed by the portable device to facilitate synchronization. Dr. Bims also fails to identify whether, or how, the execution of program code is caused by a communication resulting from user interaction with the terminal IUI, which leads to an alleged synchronization process.

c. Abbott in Combination with DUKPT Does Not Disclose "Facilitat[ing] Synchronizing Content on the Portable Device with Content on the Communications Network Node"

412. As I discussed in Section IX.C.ii.b above, I disagree with Dr. Bims that it would have been obvious for a POSITA to use DUKPT techniques in connection with the use of the encryption keys and techniques disclosed in Abbott. Therefore, it would not have been obvious for a POSITA to use DUKPT in combination with Abbott to result in execution of fourth program code by the portable device processor in response to a communication received by the portable device in response to user interaction with the claimed IUI, to cause a communication to be transmitted to a communications network node to facilitate the synchronization of content on a portable device with content on the communications network node.

of firmware updates that was an "offline upgrade, not [an] online upgrade." [*Id.* 79:23-80:1]. That alternate method meant that "all the firmware files were encapsulated inside the binary file that performed the FFU. So the interaction is only between the application and the DiskOnKey. No need to interact with external server … because all the firmware files exist inside the application." [*Id.* at 80:4-9].

436. Dr. Bims next asserts that the DiskOnKey allows for communication of a serial number and firmware version to the host computer, "both as part of the DiskOnKey's firmware and the DiskOnKey SDK." [Bims 865-67]. But Dr. Bims provides no evidence that any such alleged firmware or SDK implementation executes code in response to a communication received as a result of user interaction it the IUI, nor that it provides such information to the host computer to "facilitat[e] communications through the terminal network communication interface to a communications network node.

e. The DiskOnKey in Combination with Other References Does Not Disclose the Element of Claim 56: Wherein the Step of Executing Fourth Program Code Stored on the Portable Device Memory Causes a Communication to be Transmitted to the Communications Network Node to Facilitate Verification of the Portable Device

437. [redacted]

[redacted]

438. [redacted]

439. [redacted]

[redacted]

440. [redacted]

[redacted]

ii. [redacted]

441. In my opinion, the DiskOnKey does not disclose "executing, in response to a communication received by the portable device resulting from user interaction with the interactive user interface, third program code stored on the portable device memory to cause a communication to be transmitted to a communications network node…[which] comprises providing the terminal with data stored on the portable device memory to facilitate the terminal to transmit a communication to the communications network node…wherein the data stored on the portable device memory comprises portable device identifier information." ['703 Patent Claim 78, 86, 90]. Dr. Bims refers to "a number of example communications" that "were communications that were facilitated by the DiskOnKey providing identifier information stored on its memory to the terminal." [Bims 921]. But the element of Claim 90 of the '969 Patent requires "executing, ***in response to a communication received by the portable device resulting from user interaction with the interactive user interface***, third program code stored on the portable device memory to cause a communication to be transmitted to a communications network node." To the extent any of Dr. Bims' examples do not involve the execution of code in response to a communication received by the portable device resulting from user interaction with the interactive user interface,

iii. The DiskOnKey Does Not Invalidate Claim 101

445. Dr. Bims treats Claim 101 of the '703 Patent as substantially identical to Claim 90, and does not rely on any arguments not already addressed in my discussion of Claim 90 above. [Bims 173-175]. As such Dr. Bims fails to disclose any opinions on how the DiskOnKey could anticipate Claim 101 of the '703 Patent. Regardless, as discussed in this report, the DiskOnKey does not anticipate any of the asserted claims.

iv. The DiskOnKey Does Not Invalidate Claim 105

446. Dr. Bims treats Claim 105 of the '703 Patent as substantially identical to Claim 56, and does not rely on any arguments not already addressed in my discussion of Claim 56 above. [Bims 173-175]. As such Dr. Bims fails to disclose any opinions on how the DiskOnKey could anticipate Claim 105 of the '703 Patent. Regardless, as discussed in this report, the DiskOnKey does not anticipate any of the asserted claims.

v. The DiskOnKey Does Not Invalidate Claim 114

447. First, I note that the DiskOnKey does not disclose the elements of Claim 104 of the '703 Patent, for substantially the same reasons as it does not disclose Claim 55 of the '703 Patent. Regardless, even if the DiskOnKey did disclose the elements of Claim 104 of the '703 Patent, which it does not, it does not disclose the additional element of Claim 114.

448. Dr. Bims first contends that during the DiskOnKey's alleged firmware update process, in response to user interaction on the computer, the DiskOnKey's processor is configured to execute code to cause a communication to be transmitted to the remote server "facilitate[s] synchronizing content on the portable device with content on the communications network node, such as the DiskOnKey's firmware version. [Bims 906-07]. I disagree.

449. First, as previously discussed, the DiskOnKey does not disclose any

communication received by the portable device resulting from user interaction with the interactive user interface and configured to cause a communication to be transmitted to the communications network node. Dr. Bims simply fails to address these necessary elements of Claim 114. Moreover, Dr. Bims has not analyzed the alleged MyKey software and therefore does not know how it works or how it implements any alleged synchronization operations that are used. For instance, it is possible that the alleged synchronization component of MyKey software has already created a manifest for the contents of the DiskOnKey before any synchronization operations occur. In such a case it would just have to check the host folder to see what contents it has. Based on this check it could then determine what files to sync and thus communicate to the DiskOnKey to read/write as necessary. In this case, there is no interaction with the IUI that causes fourth program code to execute on the portable device to cause any communication to be sent.

454. Second, Dr. Bims cannot prove that the alleged synchronization over a network is even possible with MyKey software. Dr. Bims has not tested the MyKey software. And nowhere in the description of the MyKey software does it say that the folder to be synchronized can be on a network. In fact the MyKey documentation states that the synchronization drive must be "***local***" to the host: "Select the folders you would like to synchronize. ***The first folder must be an existing local folder***. The second folder must be an existing DiskOnKey folder." [INGEN-0100391 at 12]. Indeed, the screenshot of the interface provided by Dr. Bims actually says, "**Host** Folder" and "DiskOnKey Folder" indicating that the folder with which to synchronize file contents is on the "**host** computer" to which the DiskOnKey is attached. [Bims 911]. Furthermore, Dr. Bims provides not explanation of what this "host computer" directory is. There is no reason to believe that "host computer" means anything other than exactly what it says—the computer that the DiskOnKey is connected to. Indeed, Figure 15, reproduced in Dr. Bims' Report on page 449,

shows an operation involving files on the "C:" drive, which is on the local host computer.

455. Dr. Bims also has not shown that there exists any fourth program code on the DiskOnKey which is configured to be executed by the portable device processor in response to a communication received by the portable device resulting from user interaction with the interactive user interface to initiate a synchronization operation. Indeed, simple file copy operations do not necessarily require program code to be executed on a thumb drive like the DiskOnKey. Even assuming that the DiskOnKey was capable of synching files in an encrypted storage area, on USB devices the decryption operations can be done entirely in hardware. In such a case, file copy operations are likely not controlled by software at all and thus Dr. Bims does not point to any program code running on the portable device during any folder synchronization operation. To the extent that Dr. Bims contends that firmware performs these operations, this is not necessarily true—many USB mass storage devices do not contain firmware. I am unaware of any hardware level analysis that Dr. Bims has performed to show the existence of code that implements any decryption operations. It is improper and unsupported to merely assume that decryption happens in software.

vi. The DiskOnKey Does Not Invalidate Claim 124

456. Dr. Bims treats Claim 124 of the '703 Patent as substantially identical to Claim 101 and Claim 90, and does not rely on any arguments not already addressed in my discussion of Claim 90 above. [Bims 173-175]. As such Dr. Bims fails to disclose any opinions on how the DiskOnKey could anticipate Claim 124 of the '703 Patent. Regardless, as discussed in this report, the DiskOnKey does not anticipate any of the asserted claims.

claim language and the art relied on by Dr. Bims is even more stark with respect to Claims 3 and 10 of the '969 Patent. Because Dr. Bims never addresses this claim element, he does not show that any of the art he relies on discloses first program code, executed by the terminal processor that is configured to "present" a means that enables two-way responsive communication between a user and a computer. Because Dr. Bims never addresses this element, Dr. Bims cannot show that Claim 3 or 10 of the '969 Patent are invalid.

468. Similarly, Claim 3 of the '969 Patent includes the wherein clause, "the communication caused to be transmitted to the communication network node facilitates verification of the portable device." I incorporate by reference my analysis of Claims 56 and 105 of the '703 Patent as described more fully above. In my opinion, none of the references identified by Dr. Bims renders Claim 3 of the '969 Patent invalid, and Dr. Bims presents no analysis to that effect beyond what he asserts in relation to Claim 105 of the '703 Patent. Because Dr. Bims never analyzes Claim 3 of the '969 Patent and because his analysis of Claim 105 of the '703 Patent is faulty, Dr. Bims has not shown that Claim 3 of the '969 Patent is invalid.

469. Claim 10 of the '969 Patent includes the wherein clause, "the communication network node comprises a database and the communication caused to be transmitted to the communication network node facilitates synchronizing content on the portable device with content on the communication network node database." The word "database" is absent from Claim 114 of the '703 Patent, and Dr. Bims fails to address this element in his analysis of Claim 114. In my opinion, none of the references identified by Dr. Bims renders Claim 10 of the '969 Patent invalid, and Dr. Bims presents no analysis to that effect beyond what he asserts in relation to Claim 114 of the '703 Patent. Because Dr. Bims never identifies a "database" to satisfy this element of Claim

10 of the '969 Patent, Dr. Bims cannot show that this claim is invalid.[12]

XI. SECONDARY CONSIDERATIONS

A. Commercial Success

470. I have reviewed Dr. Bims's opinions regarding commercial success. I disagree with Dr. Bims for at least the following reasons.

471. I understand that evidence is needed to address commercial success for the product resulted from the claimed invention, which Dr. Bims also recognizes. [Bims, 943]. I understand that infringing products sold by PayPal and Ingenico are highly-successful commercial products that practice one or more claims of the Patents-in-Suit.

472. First, infringing products by PayPal and Ingenico practice the accused claims of Patents-in-Suit. I have opined in my previous infringement reports that infringing PayPal and Ingenico products, including but not limited to PayPal's Zettle card readers, Chip and Card Readers, etc., and Ingenico's RP750x readers, RP457c readers, etc., practice both the '703 and '969 patents.

473. Second, infringing products by PayPal and Ingenico rely significantly on the teachings of Patents-in-Suit. Accused PayPal and Ingenico products include a portable device and a terminal described in the '703 and '969 patents, the portable device being a card reader device, and the terminal being a smartphone or a similar device that is capable of connecting to accused card reader devices, and running card reader-related application. The portable device contains a third program code and a fourth program code; the terminal contains an interactive user interface, a first program code, and a second program code taught by '703 and '969 patents. Accused portable devices also execute fourth program code that causes a communication to be transmitted to a

[12] To the extent Dr. Bims contends that his summary reliance on Mr. Geier's opinions remedies this issue, I disagree.